JS 44 (Rev. 06/17)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

TASHICA FULTON-GREEN, on behalf of herself and all others similarly situated,

(b) County of Residence of First Listed Plaintiff Bucks County
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Charles E. Schaffer, Levin Sedran & Berman, 510 Walnut Street, Suite 500, Philadelphia, PA 19106, (215) 592-1500

DEFENDANTS

ACCOLADE, INC.

County of Residence of First Listed Defendant New Castle County
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☒ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☒ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☒ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing *(Do not cite jurisdictional statutes unless diversity)*:
28 U.S.C. Section 1332(d)

Brief description of cause:
Data disclosure of personal identify information

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P.

DEMAND $ 5,000,000.00

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE
01/22/2018

SIGNATURE OF ATTORNEY OF RECORD

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF PENNSYLVANIA — DESIGNATION FORM to be used by counsel to indicate the category of the case for the purpose of assignment to appropriate calendar.

Address of Plaintiff: 574 A Rosalie Street, Philadelphia, PA 19120

Address of Defendant: 251 Little Falls Drive, Wilmington, DE 19808

Place of Accident, Incident or Transaction: Philadelphia, PA
(Use Reverse Side For Additional Space)

Does this civil action involve a nongovernmental corporate party with any parent corporation and any publicly held corporation owning 10% or more of its stock?
(Attach two copies of the Disclosure Statement Form in accordance with Fed.R.Civ.P. 7.1(a)) Yes☐ No☒

Does this case involve multidistrict litigation possibilities? Yes☐ No☒

RELATED CASE, IF ANY:

Case Number: _____ Judge _____ Date Terminated: _____

Civil cases are deemed related when yes is answered to any of the following questions:

1. Is this case related to property included in an earlier numbered suit pending or within one year previously terminated action in this court? Yes☐ No☒
2. Does this case involve the same issue of fact or grow out of the same transaction as a prior suit pending or within one year previously terminated action in this court? Yes☐ No☒
3. Does this case involve the validity or infringement of a patent already in suit or any earlier numbered case pending or within one year previously terminated action in this court? Yes☐ No☒
4. Is this case a second or successive habeas corpus, social security appeal, or pro se civil rights case filed by the same individual? Yes☐ No☒

CIVIL: (Place ✔ in ONE CATEGORY ONLY)

A. *Federal Question Cases:*

1. ☐ Indemnity Contract, Marine Contract, and All Other Contracts
2. ☐ FELA
3. ☐ Jones Act-Personal Injury
4. ☐ Antitrust
5. ☐ Patent
6. ☐ Labor-Management Relations
7. ☐ Civil Rights
8. ☐ Habeas Corpus
9. ☐ Securities Act(s) Cases
10. ☐ Social Security Review Cases
11. ☐ All other Federal Question Cases
(Please specify) _____

B. *Diversity Jurisdiction Cases:*

1. ☐ Insurance Contract and Other Contracts
2. ☐ Airplane Personal Injury
3. ☐ Assault, Defamation
4. ☐ Marine Personal Injury
5. ☐ Motor Vehicle Personal Injury
6. ☒ Other Personal Injury (Please specify)
7. ☐ Products Liability
8. ☐ Products Liability — Asbestos
9. ☐ All other Diversity Cases
(Please specify) _____

ARBITRATION CERTIFICATION

(Check Appropriate Category)

I, Charles E. Schaffer, counsel of record do hereby certify:

☒ Pursuant to Local Civil Rule 53.2, Section 3(c)(2), that to the best of my knowledge and belief, the damages recoverable in this civil action case exceed the sum of $150,000.00 exclusive of interest and costs;

☒ Relief other than monetary damages is sought.

DATE: 01/22/2018 _____ 76259
Attorney-at-Law Attorney I.D.#

NOTE: A trial de novo will be a trial by jury only if there has been compliance with F.R.C.P. 38.

I certify that, to my knowledge, the within case is not related to any case now pending or within one year previously terminated action in this court except as noted above.

DATE: 01/22/2018 _____ 76259
Attorney-at-Law Attorney I.D.#

CIV. 609 (5/2012)

UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF PENNSYLVANIA — DESIGNATION FORM to be used by counsel to indicate the category of the case **for the purpose of assignment to appropriate calendar.**

Address of Plaintiff: 574 A Rosalie Street, Philadelphia, PA 19120

Address of Defendant: 251 Little Falls Drive, Wilmington, DE 19808

Place of Accident, Incident or Transaction: Philadelphia, PA
(Use Reverse Side For Additional Space)

Does this civil action involve a nongovernmental corporate party with any parent corporation and any publicly held corporation owning 10% or more of its stock?
(Attach two copies of the Disclosure Statement Form in accordance with Fed.R.Civ.P. 7.1(a)) Yes☐ No☒

Does this case involve multidistrict litigation possibilities? Yes☐ No☒

RELATED CASE, IF ANY:

Case Number: _____ Judge _____ Date Terminated: _____

Civil cases are deemed related when yes is answered to any of the following questions:

1. Is this case related to property included in an earlier numbered suit pending or within one year previously terminated action in this court? Yes☐ No☒
2. Does this case involve the same issue of fact or grow out of the same transaction as a prior suit pending or within one year previously terminated action in this court? Yes☐ No☒
3. Does this case involve the validity or infringement of a patent already in suit or any earlier numbered case pending or within one year previously terminated action in this court? Yes☐ No☒
4. Is this case a second or successive habeas corpus, social security appeal, or pro se civil rights case filed by the same individual? Yes☐ No☒

CIVIL: (Place ✔ in ONE CATEGORY ONLY)

A. *Federal Question Cases:*

1. ☐ Indemnity Contract, Marine Contract, and All Other Contracts
2. ☐ FELA
3. ☐ Jones Act-Personal Injury
4. ☐ Antitrust
5. ☐ Patent
6. ☐ Labor-Management Relations
7. ☐ Civil Rights
8. ☐ Habeas Corpus
9. ☐ Securities Act(s) Cases
10. ☐ Social Security Review Cases
11. ☐ All other Federal Question Cases
(Please specify) _____

B. *Diversity Jurisdiction Cases:*

1. ☐ Insurance Contract and Other Contracts
2. ☐ Airplane Personal Injury
3. ☐ Assault, Defamation
4. ☐ Marine Personal Injury
5. ☐ Motor Vehicle Personal Injury
6. ☒ Other Personal Injury (Please specify)
7. ☐ Products Liability
8. ☐ Products Liability — Asbestos
9. ☐ All other Diversity Cases
(Please specify) _____

ARBITRATION CERTIFICATION

(Check Appropriate Category)

I, Charles E. Schaffer, counsel of record do hereby certify:

☒ Pursuant to Local Civil Rule 53.2, Section 3(c)(2), that to the best of my knowledge and belief, the damages recoverable in this civil action case exceed the sum of $150,000.00 exclusive of interest and costs;

☒ Relief other than monetary damages is sought.

DATE: 01/22/2018 _____ 76259
Attorney-at-Law Attorney I.D.#

NOTE: A trial de novo will be a trial by jury only if there has been compliance with F.R.C.P. 38.

I certify that, to my knowledge, the within case is not related to any case now pending or within one year previously terminated action in this court except as noted above.

DATE: 01/22/2018 _____ 76259
Attorney-at-Law Attorney I.D.#

CIV. 609 (5/2012)

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

CASE MANAGEMENT TRACK DESIGNATION FORM

TASHICA FULTON-GREEN, on behalf of herself and all others similarly situated, v. ACCOLADE, INC.	CIVIL ACTION
	NO.

In accordance with the Civil Justice Expense and Delay Reduction Plan of this court, counsel for plaintiff shall complete a Case Management Track Designation Form in all civil cases at the time of filing the complaint and serve a copy on all defendants. (See § 1:03 of the plan set forth on the reverse side of this form.) In the event that a defendant does not agree with the plaintiff regarding said designation, that defendant shall, with its first appearance, submit to the clerk of court and serve on the plaintiff and all other parties, a Case Management Track Designation Form specifying the track to which that defendant believes the case should be assigned.

SELECT ONE OF THE FOLLOWING CASE MANAGEMENT TRACKS:

(a) Habeas Corpus – Cases brought under 28 U.S.C. § 2241 through § 2255. ( )

(b) Social Security – Cases requesting review of a decision of the Secretary of Health and Human Services denying plaintiff Social Security Benefits. ( )

(c) Arbitration – Cases required to be designated for arbitration under Local Civil Rule 53.2. ( )

(d) Asbestos – Cases involving claims for personal injury or property damage from exposure to asbestos. ( )

(e) Special Management – Cases that do not fall into tracks (a) through (d) that are commonly referred to as complex and that need special or intense management by the court. (See reverse side of this form for a detailed explanation of special management cases.) (X)

(f) Standard Management – Cases that do not fall into any one of the other tracks. ( )

01/22/2018	Charles E. Schaffer	Plaintiff, Tashica Fulton-Green
Date	**Attorney-at-law**	**Attorney for**
(215) 592-1500	(215) 592-4663	cschaffer@lfsblaw.com
Telephone	**FAX Number**	**E-Mail Address**

(Civ. 660) 10/02

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

TASHICA FULTON-GREEN, on behalf of herself and all others similarly situated, Plaintiff, v. ACCOLADE, INC., Defendant.	Civil Action No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Tashica Fulton-Green, individually and on behalf of all others similarly situated, by and through counsel, brings this action against Defendant Accolade (hereafter referred to as "Defendant"), and allege as follows based upon personal knowledge, investigation of counsel, and information and belief:

NATURE OF THE ACTION

1. This class action arises from Accolade's voluntary failure to adequately safeguard and protect the highly confidential and sensitive, personally-identifiable information ("PII"), including social security and W-2 information, of its own current and former employees. Plaintiff, on behalf of herself and other current and former Accolade employees who had their PII wrongfully and voluntarily disseminated by Defendant to a third-party or parties, seeks to recover for the substantial damages that have been caused, and will continue to be caused, by Defendant's flagrant violations of their rights, and the insufficient remedy afforded by Defendant.

2. Defendant Accolade is an on-demand healthcare concierge for employers, health plans and health systems. According to its own website, Accolade has "been recognized as one of the nation's 25 most promising companies by Forbes magazine, the fastest-growing private healthcare company by Inc. 500, and a top workplace five years running."[1]

3. Accolade employs individuals in Arizona, Washington, and Pennsylvania.

4. Although Accolade touts its high-tech advocacy on behalf of its clients, it cannot say the same about all of its employees. On January 19, 2017, an Accolade Human Resources ("HR") employee disseminated and disclosed unencrypted PII—including the names, addresses, social security numbers, earnings information, and other highly sensitive information—of current and former Accolade employees to a third-party who requested such information via an e-mail (the "Data Disclosure"). The Accolade employee did not bother to confirm or authenticate the validity of the request prior to sending the highly sensitive and confidential PII of Plaintiff and the Class Members to the third-party. Indeed, despite being placed on ample notice of the risks of such data breaches, Accolade failed to implement the most basic security precautions or checks before releasing its own employees' PII.

5. Social security numbers and salary information are entitled to a particularly high level of protection due to their sensitive and confidential nature. The combination of this information with other identifying information, such as the names and addresses of employees, enhanced the sensitivity of the information made susceptible to abuse and exploitation, and required the utmost protection in its handling. Accolade knew and understood the confidential and private nature of Plaintiff's and the Class Members' PII, and owed duties to Plaintiff and the Class

[1] https://www.accolade.com/about-us/

Members to protect and maintain the confidentiality of their PII. In particular, social security numbers are perhaps the most important piece of information to an individual, and are not easily replaced. Unlawful exploitation of social security numbers costs the federal government hundreds of millions of dollars each year from the fraudulent filing of tax returns by identity thieves, not to mention the harms suffered by persons whose social security numbers are stolen and/or misappropriated.

6. It is well-known, and the subject of many media reports, that PII data is highly coveted by, and the frequent target of, hackers and cybercriminals. Legitimate organizations and the criminal underground alike recognize the value in PII. Otherwise, they wouldn't pay for it or aggressively seek it. PII data has been stolen and sold by the criminal underground on many occasions in the past, and the accounts of the thefts and unauthorized access have been the subject of many media reports. In recent years, criminals have increasingly been drawn to unlawfully obtaining PII because they can use biographical data from multiple sources to perpetuate more and larger thefts.[2] Illicitly obtained PII, sometimes aggregated from different breaches, is sold on the black market, including on websites.[3] In turn, identity thieves can use PII, *inter alia*, to open new financial accounts and incur charges in another person's name, take out loans in another person's name, incur charges on existing accounts, clone ATM, debit, or credit cards, obtain a job or housing, and commit various types of government crimes such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, and filing a fraudulent tax return using the

---

[2] *See* Verizon 2014 PCI Compliance Report, Verizon, http://www.verizonenterprise.com /resources/reports/rp_pci-report-2014_en_xg.pdf (last visited December 8, 2017).

[3] *See, e.g.*, *How Much Is Your Identity Worth?*, Krebs on Security, http://krebsonsecurity.com /2011/11/how-much-is-your-identity-worth/ (last visited December 8, 2017).

victim's information to obtain a fraudulent refund. Worse yet, some of this activity may not come to light for years, and may continue in perpetuity.

7. On or about January 20, 2017, Accolade notified its employees that on January 19, 2017, it discovered that an Accolade employee fell for a well-known and warned about "phishing" scheme two days earlier by complying with an email request from a cybercriminal who was masquerading as an authorized third party working with Accolade to send employees' W-2s and other personal information as part of Accolades' business operation to that party. This resulted in the unauthorized disclosure of all U.S-based employees' W-2 forms including sensitive personally identifying information ("PII") like employees' names, addresses, Social Security Numbers, salaries and taxes withheld for 2016 to an unauthorized third-party ("the Data Disclosure"). Accolade notified its employees via email of the Data Disclosure, encouraging employees to remain vigilant to the possibility of fraud and identity theft, and offering them free credit monitoring for two years.

8. Due to Accolade's failure to implement the most basic of safeguards and precautions, the most sensitive data of Accolade's current and former employees, including social security numbers, W-2 information, and other PII, is now in the possession of an unknown third-party or parties who have already used the PII for illegal purposes, and will be able to continue doing so indefinitely. This unauthorized third-party or parties gained access to the PII of Plaintiff and the Class Members for the purpose of using the information for improper and unlawful purposes, including identity theft, the filing of false tax returns, and the submission of fraudulent student loan applications and fraudulent credit applications.

9. As a direct and proximate result of Accolade's failure to maintain adequate and reasonable data security processes, controls, policies, procedures, and protocols to safeguard and

protect the PII of its employees—and despite numerous, repeated warnings from the Internal Revenue Service ("IRS") and Federal Bureau of Investigation ("FBI") regarding the imminent risks of this precise issue, the well-publicized data breaches that have occurred recently nationwide, Plaintiff and the Class Members have had their PII compromised and have suffered substantial harm from the misuse of their PII . Plaintiff and the Class Members have had their PII compromised and have suffered substantial harm from the misuse of their PII. Plaintiff and the Class Members have been placed at risk of current and future fraud, identity theft, and financial injury, and have incurred direct and significant financial and temporal expenses that they will continue to incur in the future, including, *inter alia*, costs associated with credit and identity theft monitoring, protection, and repair, replacement and repair of compromised financial information, and other measures needed to protect against and resolve the misuse of their PII.

10. Upon information and belief, Class Members have been required to take the time, which they otherwise would have dedicated to other life demands (such as work), and effort to mitigate the actual and potential impact of the Data Disclosure on their lives. Such acts of mitigation may include, *inter alia*; placing "freezes" and "alerts" with credit reporting agencies and incurring the costs associated therewith, as well as the costs associated with lifting any freezes or removing any alerts for legitimate purchases or extensions of credit, contacting their financial institutions, closing or modifying financial accounts, scheduling and attending appointments with the IRS, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured.

11. No one can know what else the cyber criminals will do with the employees' PII. However, what is known is that Accolade's U.S.-based employees are now, and for the rest of their lives will be, at a heightened risk of further identity theft and fraud. In addition, the disclosure of

the PII results to unauthorized recipients such as cybercriminals results in the devaluation of this otherwise valuable personable information and asset. Marketplaces exit where consumers such as Class Members can directly sell access to their personal information. In addition, third party(s) have created marketplaces for the buying and selling of consumers PII, e.g. (we should give some examples).

12. Credit bureaus are permitted to, and do, sell consumers' personal and private financial information to any and all lenders both in the US and overseas.[4] The financial information credit bureaus sell includes consumers' names, addresses, phone numbers, credit scores, current debt, debt history, property information, ages, genders and estimated incomes.[5]

13. As summarized in one consumer credit publication, these credit bureaus collect, market and sell PII for four general purposes:[6]

a. Consumer initiated report and scores
b. Lender initiated account reviews
c. Lender initiated prescreens and triggers
d. Traditional business initiated demographics

14. The value of PII is not limited to those who seek to use it for a lawful purpose but extends to criminals as well. According to one report, in 2015, the median price for a person's PII

[4] *See Credit Bureaus Are Selling Your Name and Private Financial Information*, http://www.skipmcgrath.com/articles/credit-bureau-selling-information.shtml (last visited December 8, 2017).
[5] *See Credit Bureaus Are Selling Your Name and Private Financial Information*, http://www.skipmcgrath.com/articles/credit-bureau-selling-information.shtml (last visited December 8, 2017).
[6] *See Do Credit Bureaus Sell Your Personal Information*? https://www.savvyoncredit.com/credit-bureaus-sell-personal-information/ (last visited December 8, 2017).

on the dark web was $21.35.[7]

15. There is no question that a consumer's PII is a valuable asset. When it is disclosed to an unauthorized recipient especially a cybercriminal the markets for this information adjust and the value of that PII to the consumer who owns it – the only person who is lawfully entitled to its full value – is reduced.

16. For all Class Members, fear and anxiety of identity theft or fraud is the new norm and their once pristine and protected PII has been devalued because of the disclosure to unauthorized recipients who are cybercriminals.

17. Plaintiff brings this class action against Accolade for failing to adequately secure and safeguard the PII of Plaintiff and the Class, for failing to comply with industry standards regarding electronic transmission of PII, and for failing to adequately notify Plaintiff and other Class members as to precisely how their sensitive personal information had been given to unknown persons and what measures were being taken to ensure future protection.

18. Accolade disregarded the rights of Plaintiff and Class members by intentionally, willfully, recklessly, and/or negligently failing to heed warnings of "phishing schemes" and take and implement adequate and reasonable measures to ensure that the data it stores was safeguarded, failing to take available steps to prevent the disclosure from happening, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data even for internal use. As the result, the PII of Plaintiff and Class Members was compromised and disclosed to an unknown and unauthorized third party. However, as this same

[7] *See Here's what your stolen identity goes for on the internet's black market*, https://qz.com/460482/heres-what-your-stolen-identity-goes-for-on-the-internets-black-market/ (last visited December 8, 2017).

information remains stored in Accolade's computer systems, upon information and belief, Plaintiff and Class members have an interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

19. Critically, Accolade is in the business of PII. It seeks the trust of its clients in providing a member experience and no doubt deals every day with clients' private health care and claims information. Protecting this information should be nothing new or exceptional to it. Rather, it should be the norm.

PARTIES

Plaintiff Tashica Fulton-Green

20. Plaintiff Tashica is a citizen and resident of Philadelphia, Pennsylvania residing at 574 A Rosalie Street, Philadelphia, Pennsylvania, 19120.

21. Plaintiff Fulton-Green started to work for Accolade as a Health Associate in April 2012. She left employment with Accolade in June 2017.

22. As part of her employment with Accolade, plaintiff was required to and did entrust her PII with them.

23. On or about January 20, 2017, while she was still employed by Accolade, Plaintiff Fulton-Green was notified that her PII was disclosed without her authorization to an unknown third party as a result of the Data Disclosure.

24. Prior to the Data Disclosure, Plaintiff Fulton-Green had no knowledge of ever being the victim of identity theft or being involved in a data breach incident or any incident in which her personal information was compromised as the result of a phishing scheme.

25. Because her personal information was disclosed as a result of the Data Disclosure, Plaintiff enrolled in the ProtectMyID Alert credit monitoring service offered by Accolade.

26. As a result of the Data Disclosure, Plaintiff has spent time and effort attempting to mitigate the dangers and continuing risk of identity theft and tax fraud. Plaintiff has spent, and will continue to spend, time monitoring her credit reports and reports issued by ProtectMyID Alert, including alerts which cause her unnecessary stress and anxiety, notifying her financial institutions of the Data Disclosure, and taking other actions necessary to protect herself from future incidents of identity theft or fraud.

27. As a result of the Data Disclosure, Plaintiff's PII has been compromised and devalued in the marketplaces which exist for PII.

Defendant

28. Defendant Accolade, Inc. is a Delaware corporation with its principal place of business in Plymouth Meeting, Pennsylvania. Accolade employs over 500 individuals across the country, including Pennsylvania, Washington, and Arizona.

JURISDICTION AND VENUE

29. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act 28 U.S.C. § 1332(d) ("CAFA"), because the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, there are more than 100 class members, and at least one class member is a citizen of a state different from Defendant and a citizen of a foreign state.

30. This Court has personal jurisdiction over Defendant because the headquarters for Accolade is in this District and Defendant conducts substantial business in the state of Pennsylvania, and in this District.

31. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because the headquarters for Accolade is in this District, Defendant regularly conducts business in this District, and a substantial part of the events or omissions giving rise to this action occurred in this District.

FACTUAL ALLEGATIONS

32. As a condition of employment, Accolade requires that employees entrust it with certain personal information. In its ordinary course of business, Accolade maintains the personal and tax information, including the name, address, zip code, date of birth, wage and withholding information, and Social Security number, of each current and former employee.

33. Plaintiff and members of the proposed Class, as current and former employers, relied on Accolade to keep this information confidential and securely maintained.

34. An individual's social security number is perhaps the most important piece of confidential and sensitive information to an individual in the modern world. Neal O'Farrell, a security and identity theft expert for Credit Sesame, calls a social security number "your secret sauce," that is "as good as your DNA to hackers." Social security numbers are used, among other things, to verify eligibility for employment, to apply for a passport, to open a bank account, or to apply for a credit card, student loan, or mortgage. A social security number is also needed to obtain government benefits like social security and Medicare. Social security numbers are assigned to citizens (and sometimes to noncitizens) as early as their birth, and are required to enroll in school and to obtain healthcare services. A social security number follows a person through life and can be used to access a person's most sensitive and confidential financial information.

35. The United States Government Accountability Office ("GAO") noted as far back as June 2007, in a report on data breaches ("GAO Report"), that identity thieves use identifying data such as social security numbers to open financial accounts, receive government benefits, and

incur charges and credit in a person's name. [8]The GAO Report states, this type of identity theft is the most harmful because it may take some time for the victim to become aware of the theft, and can adversely impact the victim's credit rating. The GAO Report also states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."

36. Identity-theft crimes often include more than just crimes of financial loss. Identity thieves can also commit various types of government fraud, such as obtaining a driver's license or official identification card in the victim's name but with the thief's picture, using the victim's name and social security number to obtain government benefits, and/or filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's social security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[9] In addition, loss of private and personal health-information can expose the victim to loss of reputation, loss of job employment, blackmail, and other negative effects.[10]

---

[8] *See Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, United States Government Accountability Office, http://www.gao.gov/new.items/d07737.pdf (last visited December 8, 2017).

[9] *See* FTC Identity Theft Website, *supra.*

[10] *See Identity Smart: A Guide For Consumers to Help Protect Against Identity Theft*, The National Crime Prevention Council, http://www.ncpc.org/resources/files/pdf/theft/NCPC-ID%20Theft.pdf (last visited December 8, 2017) (stating that identity thieves "may threaten national security or commit acts of terrorism" and noting that the September 11 hijackers used fake ID's to board their planes); *see also* Bob Sullivan, *9/11 report light on ID theft issues*, NBC NEWS, http://www.nbcnews.com/id/5594385 (last visited December 8, 2017) (stating that the September 11 hijackers "liberally used document fraud prior to that date, some to ease entrance into the United States, others to move around once they were here and to obtain drivers' licenses they needed to board the airplanes").

37. The theft of social security numbers in particular, as opposed to other PII, is difficult to rectify because a person whose personal information has been compromised may not see any signs of identity theft for years, social security numbers are difficult to change, and their misuse can continue for years into the future. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

38. Sensitive PII information, such as social security numbers, is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for a number of years.[11] As a result of recent large-scale data breaches and disclosures, identity thieves and cyber criminals have openly posted stolen credit card numbers, social security numbers, and other sensitive information directly on various, internet websites making the information publicly available. In one study, researchers found hundreds of websites displaying stolen, sensitive information. Strikingly, none of these websites were blocked by Google's safeguard filtering mechanism—the "Safe Browsing list." The study concluded:

> It is clear from the current state of the credit card black-market that cyber criminals can operate much too easily on the Internet. They are not afraid to put out their email addresses, in some cases phone numbers and other credentials in their advertisements. It seems that

[11] Companies, in fact, also recognize Sensitive Information as an extremely valuable commodity akin to a form of personal property. For example, Symantec Corporation's Norton brand has created a software application that values a person's identity on the black market. *See Every Click Matters*, Norton by Symantec, https://community.norton.com /en/blogs/symantec-cyber-education/every-click-matters (last visited October 5, 2017); *see also* T. Soma, *et al.*, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3–*4 (2009).

> the black market for cyber criminals is not underground at all. In fact, it's very "in your face."[12]

39. A similar, recent report about healthcare-related identity-theft fraud, sponsored by Experian, indicated that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000."[13]

40. The unauthorized disclosure of a person's social security number can be particularly damaging since social security numbers cannot be easily replaced like a credit card or debit card. A person whose PII has been compromised cannot obtain a new social security number unless he or she can show that the number is being used fraudulently.

41. Even if a victim were to obtain a new social security number, that would not absolutely prevent against identity theft. Government agencies, private businesses, and credit reporting companies likely maintain a victim's records under the old number, so using a new social security number will not guarantee a fresh start. For some identity-theft and identity-fraud victims, a new number may create new problems. Because prior, positive credit information is not associated with the new social security number, it is more difficult to obtain credit due to the absence of a credit history. Indeed, the Social Security Administration warns that "a new number probably won't solve all [] problems . . ." and "won't guarantee [] a fresh start."[14]

42. A person whose PII has been compromised may experience identity theft and identity fraud for years because PII is a valuable commodity to identity thieves, and once that

---

[12] *See The "Underground" Credit Card Blackmarket*, Stop The Hacker, http://www.stopthe hacker.com/2010/03/03/the-underground-credit-card-blackmarket/ (last visited December 8, 2017).
[13] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET, http://news.cnet.com/8301-27080_3-10460902-245.html (last visited December 8, 2017).
[14] *See Identity Theft and Your Social Security Number*, Social Security Administration, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited December 8, 2017).

information has been compromised, these criminals often trade the information on the "cyber black-market" for years, and possibly indefinitely.

43. A "phishing" scheme is an attempt to acquire personal information, such as usernames, passwords, credit card details, and other sensitive information, by masquerading as a trustworthy entity or individual through an electronic communication, such as e-mail. A "whaling" scheme—otherwise known as "CEO fraud" or "fake president fraud"—is a variation of a "phishing" scheme. A "whaling" scheme specifically targets or impersonates high-ranking members of a company, with the usual goal being to trick the contacted employee into sending sensitive or personal information via an unsecure channel, such as e-mail

44. During tax season, cybercriminals often use phishing or whaling attacks to steal W-2 data, which, in turn, is used in connection with tax-refund fraud. Cybercriminals may also sell the information underground (i.e., on the dark web) or use it to stage further attacks.

45. On or about January 20, 2017, Accolade notified its employees that it was "a victim of a phishing scheme that included a targeted email sent on Tuesday, January 17 to our team, requesting employee W-2s."

46. The email stated that the employees' 2016 W-2 tax information, including names, addresses, social security numbers, salary and taxes withheld for 2016, had been involved in the disclosure.

47. This Data Disclosure occurred at a time in the calendar year when W-2 information is most vital and valuable.

48. In fact, Accolade acknowledged the risk of fraudulent tax returns in its notice to employees.

49. The January 20, 2017 email from Accolade also notified employees that the

company would be providing two years of credit monitoring services provided by Experian. Employees were given until January 29, 2019 to enroll for the service.

50. Accolade could have prevented this Data Disclosure and was not without warning of such phishing email scams, yet it failed to implement adequate measures to protect its employees' PII.

51. The risk of theft by, or disclosure to, cyber criminals of sensitive data, including PII, stored electronically is well-documented and common knowledge. In the information age, such attacks are commonplace and thus companies such as Accolade are, and/or should be, aware that they must take precautions to prevent becoming unwitting accomplices to these schemes, especially in light of numerous recent, high-profile attacks.

52. Indeed, companies nationwide, including various retailers, banks, hospitals, and other high-profile businesses, have been hit by highly-publicized phishing and whaling schemes in recent times.

53. Since the beginning of 2016, the following companies have publicized similar data breaches in which their employees' W-2 information was compromised and disclosed as a result of similar phishing scams: A&A Ready Mixed Concrete, Academy of Art Institute, Acronis, Actifio Inc., Advance Auto Parts, Agenus, Alpha Payroll Services, American Type Culture Collection, AmeriPride Services Inc., Applied Systems Inc., ARC International, ARIAD Pharmaceuticals, Ash Brokerage Corp., Aspect Software, ASPIRAnet, Asure Software, Astreya Partners, Inc., Avendra, LLC, Avention (now Dun & Bradstreet (D&B)), Avinger, Inc., AxoGen, Inc., BackOffice Associates, Behavioral Science Technology, Ben Bridge Jeweler, Inc., Billy Casper Golf, BloomReach, BrightView, Bristol Farms, Brunswick Corporation (Brunswick Boat Group, Boston Whaler, Cybex International, Leiserv Inc., and Sea Ray Boats, Inc.), Care.com (and

its subsidiaries), CareCentrix, Central Concrete Supply Co. (Right Away Redy Mix and Rock Transport, Inc.), Century Fence, Champlain Oil, Client Network Services, ConvaTec Inc., Convey Health Solutions, Conway Group, Crane Co., Dare Enterprises (via Blue Belt Technologies), DataXu Inc., DealerSocket Inc., Dennis Group, Digilant, Dixie Group, Dynamic Aviation, eClinicalWorks, EMSI (Examination Management Services, Inc.), Endologix Inc., EPTAM Plastics, Equian, LLC, Evening Post Industries, Fast Company, Foss Manufacturing Company, Gamesa Wind US, General Communication, Inc. (GCI, Denali Media, UUI, and Unicom), Gryphon Technologies, Haeco Americas LLC, I.M. Systems Group, IASIS HEALTHCARE LLC, Information Innovators Inc., Information Resources Inc., InvenSense, InVentiv Health, Inc., ISCO Industries, J. Polep Distribution Services, Kantar Group, Krispy Kreme, Lamps Plus and Pacific Coast Lighting, Land Title Guarantee Company, Lanyon Solutions, LAZ Parking, Magnolia Health Corporation, Main Line Health, Management Health Systems d/b/a MedPro Healthcare Staffing, Mansueto Ventures (on behalf of Inc.), Maritz Holdings, Inc., Masy Bioservices, Matric NAC and Matrix Service Company, MCM Staffing, Medieval Times, Mercy Housing, Inc., Michels Corporation, Mitchell International Inc., Milwaukee Bucks, MNP Corporation (on behalf of its affiliate, General Fasteners Company), Monarch Beverage Company, Moneytree, Morongo Casino, Nation's Lending Corporation, NetBrain Technologies, Inc., Netcracker Technology, New Leaders, NTT Data, O.C. Tanner, OpSec Security, PerkinElmer, Pharm-Olam International, Pivotal Software, Inc., Polycom, Primary Residential Mortgage, Inc. (PRMI), Proskauer Rose, Puppet, Inc., Pure Integration, LLC, QTI Group, RagingWire Data, Rightside, RugDoctor, Ryman Hospitality Properties (Grand Ole Opry, WSM-AM, and Wildhorse Saloon Nashville's General Jackson Showboat), SalientCRGT, Santa Rosa Consulting, Seagate Technology, SevOne, Silicon Laboratories, Single Digits, Snapchat, Spectrum, Inc., Sprouts, Tom McLeod Software Corps,

Total Community Options Inc. d/b/a InnovAge, Turner Construction, VBrick Systems, Verity Health System, Veterans Management Services, Inc., Whiting-Turner Contracting Company, WorkCare, Wynden Stark, d/b/a GQR Global Markets/City Internships, York Hospital, and YourEncore.[15]

54. In light of these well-documented data breaches, Accolade knew, or should have known, that it was susceptible to such an attack, and that it needed to implement and maintain adequate and reasonable data security processes, controls, policies, procedures, and protocols to safeguard and protect the sensitive and confidential information with which it was entrusted.

55. Accolade's negligence in safeguarding its employees' PII is exacerbated by the repeated warnings and alerts, not only of the increasing risk of general email scams, but of the actual W-2 phishing email scam it chose to ignore and, thus, fell prey to. The IRS and the FBI have published warnings over the last several years regarding the prevalence of malicious phishing e-mails being sent to individuals and companies to steal personal information.

56. On August 27, 2015, the Federal Bureau of Investigation ("FBI") issued a report warning of the increasingly common scam, known as Business Email Compromise, in which companies had fallen victim to phishing emails.[16] Most importantly, this report called attention to the significant spike in scams, also referred to as spoofing, in which cyber criminals send emails that appear to have initiated from the CEO or other top-level executive at the target company.

---

[15] *See Meanwhile, back at the phishing for W-2 department ...* https://www.databreaches.net/meanwhile-back-at-the-phishing-for-w-2-department/ (last visited December 8, 2017).

[16] *See, Public Service Announcement, Business Email Compromise*, Alert No. I-082715a-PSA (August 27, 2015), *available at* https://www.ic3.gov/media/2015/150827-1.aspx (last visited December 8, 2017).

57. Business Email Compromise or spoofing is the forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source. For example, spoofed email may purport to be from someone in a position of authority within a company asking for sensitive data such as passwords or employee information that can be used for a variety of criminal purposes. A telltale sign of a spoofing e-mail is an "urgent" request from a company "executive" requesting that confidential information be provided via email.

58. As noted by cybersecurity journalist Brian Krebs, this type of fraud "usually begins with the thieves either phishing an executive and gaining access to that individual's email account or emailing employees from a look-alike domain that is one or two letters off from the company's true domain name." [17]

59. Spoofing fraud has been steady increasing in recent years. The FBI recently issued an alert stating that from October 2013 through February 2016, law enforcement received reports from over 17,000 victims of "spoofing" scams, which resulted in more than $2.3 billion in losses. Since January 2015, the FBI has seen a 270% increase in identified victims and exposed loss from spoofing scams.[18]

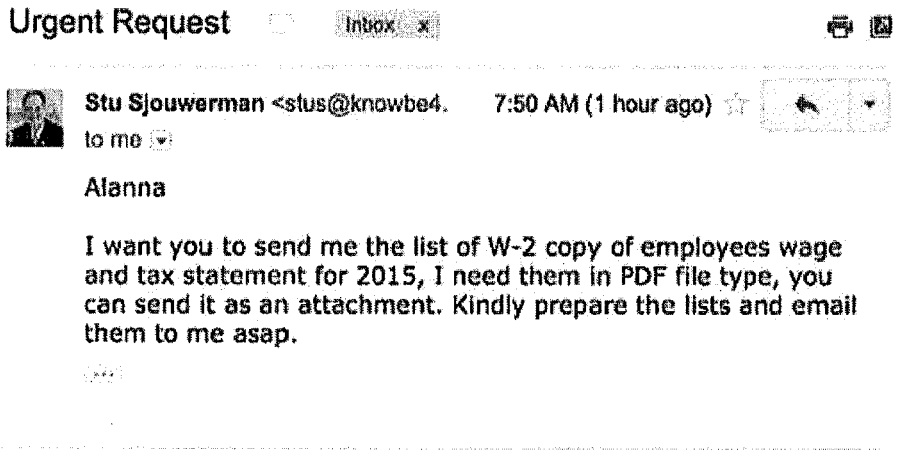
60. Companies can mount two primary defenses to spoofing scams: employee education and technical security barriers. Employee education is the process of adequately making employees aware of common spoofing scams and implementing company-wide policies requiring the request or transfer of sensitive personal or financial information only through secure sources to known recipients. Employee education and secure file-transfer protocols provide the easiest

[17] Brian Krebs, *FBI: $2.3 Billion Lost to CEO Email Scams*, KREBS ON SECURITY (April 7, 2016), *available at* http://krebsonsecurity.com/2016/04/fbi-2-3-billion-lost-to-ceo-email-scams/ (last visited December 31, 2016).
[18] *FBI Warns of Dramatic Increase in Business E-Mail Scams* (April 4, 2016), *available at* https://www.fbi.gov/phoenix/press-releases/2016/fbi-warns-of-dramatic-increase-in-business-email-scams (last visited December 31, 2016).

method to assist employees in properly identifying fraudulent e-mails and prevent unauthorized access of personal and tax information.

61. From a technical perspective, companies can also greatly reduce the flow of spoofing e-mails by implementing certain security measures governing e-mail transmissions. Companies can use a simple email validation system that allows domain owners to publish a list of IP addresses that are authorized to send email on their behalf to reduce the amount of spam and fraud by making it much harder for malicious senders to disguise their identities. Companies can also use email authentication that blocks email streams that have not been properly authenticated.

62. On February 24, 2016, cybersecurity journalist Brian Krebs warned of the precise scam which snared Accolade in a blog that said all it needed to say in its title: Phishers Spoof CEO, Request W2 Forms.[19] Krebs warned that cybercriminals were attempting to scam companies by sending false emails, purportedly from the company's chief executive officer, to individuals in the human resources or accounting department asking for copies of W-2 data for all employees. Krebs even provided an example of such an email that had been sent to another company:



[19] Brian Krebs, *Phishers Spoof CEO, Request W2 Forms*, KREBS ON SECURITY *available at* http://krebsonsecurity.com/2016/02/phishers-spoof-ceo-request-w2-forms/ (last visited December 30, 2016).

63. Further, on March 1, 2016, the IRS issued an alert to payroll and human resources professionals warning of the same scheme. In precise detail, the alert stated:

> The Internal Revenue Service today issued an alert to payroll and human resources professionals to beware of an emerging phishing email scheme that purports to be from company executives and requests personal information on employees.
>
> The IRS has learned this scheme — part of the surge in phishing emails seen this year — already has claimed several victims as payroll and human resources offices mistakenly email payroll data including Forms W-2 that contain Social Security numbers and other personally identifiable information to cybercriminals posing as company executives.
>
> "This is a new twist on an old scheme using the cover of the tax season and W-2 filings to try tricking people into sharing personal data. Now the criminals are focusing their schemes on company payroll departments," said IRS Commissioner John Koskinen. "If your CEO appears to be emailing you for a list of company employees, check it out before you respond. Everyone has a responsibility to remain diligent about confirming the identity of people requesting personal information about employees." [20]

64. On February 18, 2016, the IRS renewed this alert for HR and Accounting professionals.

65. On April 4, 2016, the FBI's Phoenix, Arizona office published a news bulletin entitled "FBI Warns of Dramatic Increase in Business E-Mail Scams," wherein it highlighted the dramatic and ever-increasing extent of e-mail fraud schemes, and the substantial effects such schemes were having on businesses and victims in each state nationwide.[15] The FBI's bulletin noted the "great lengths" schemers go to in perpetrating their fraudulent schemes, highlighted the 270% increase in identified victims and exposed losses resulting from such schemes, and provided resources and tips for businesses to protect themselves, including exercising greater scrutiny of e-mail requests, making telephone calls

[20] IRS, *IRS Alerts Payroll and HR Professionals to Phishing Scheme Involving W-2s*, IR-2016-34 (March 1, 2016), *available at* https://www.irs.gov/uac/Newsroom/IRS-Alerts-Payroll-and-HR-Professionals-to-Phishing-Scheme-Involving-W2s (last visited December 30, 2016).

to verify e-mail requests, and practicing multi-level authentication.

66. On June 14, 2016, the FBI issued another PSA entitled "Business E-Mail Compromise: The 3.1 Billion Dollar Scam."[21] This PSA noted that the Business E-mail Compromise ("BEC") scheme "continues to grow, evolve, and target businesses of all sizes," and critically identified a "new" BEC scenario presenting a distinct risk to businesses—Data Theft involving PII and W-2 information—which "first appeared just prior to the 2016 tax season." To that end, the FBI warned:

> Based on [Internet Crime Complaint Center] complaints and other complaint data, there are five main scenarios by which this scam is perpetrated. BEC victims recently reported a new scenario (Data Theft) involving the receipt of fraudulent e-mails requesting either all Wage or Tax Statement (W-2) forms or a company list of Personally Identifiable Information (PII). * * *
>
> **Scenario 5 (New): Data Theft**
> Fraudulent requests are sent utilizing a business executive's compromised e-mail. The entity in the business organization responsible for W-2s or maintaining PII, such as the human resources department, bookkeeping, or auditing section, have frequently been identified as the targeted recipient of the fraudulent request for W-2 and/or PII. Some of these incidents are isolated and some occur prior to a fraudulent wire transfer request. Victims report they have fallen for this new BEC scenario, even if they were able to successfully identify and avoid the traditional BEC incident. The data theft scenario (Scenario 5) of the BEC first appeared just prior to the 2016 tax season.

Regarding "suggestions for protection and best practices," the FBI specifically recommended that businesses take the following steps to prevent falling victim to e-mail fraud schemes:

> Businesses with an increased awareness and understanding of the BEC scam are more likely to recognize when they have been targeted by BEC fraudsters, and are therefore more likely to avoid falling victim and sending fraudulent payments.
>
> Businesses that deploy robust internal prevention techniques at all levels (especially targeting front line employees who may be the recipients of initial phishing attempts), have proven highly successful in recognizing and deflecting BEC attempts.

[21] See Business E-Mail Compromise: The 3.1 Billion Dollar Scam, Federal Bureau of Investigation, https://www.ic3.gov/media/2016/160614.aspx (last visited October 10, 2017).

Some financial institutions reported holding their customer requests for international wire transfers for an additional period of time, to verify the legitimacy of the request.

The following is a compilation of self protection strategies provided in the BEC PSAs from 2015.

- Avoid free web-based e-mail accounts: Establish a company domain name and use it to establish company e-mail accounts in lieu of free, web-based accounts.

- Be careful what is posted to social media and company websites, especially job duties/descriptions, hierarchal information, and out of office details.

- Be suspicious of requests for secrecy or pressure to take action quickly.

- Consider additional IT and financial security procedures, including the implementation of a 2-step verification process. For example –
  - o Out of Band Communication: Establish other communication channels, such as telephone calls, to verify significant transactions. Arrange this second-factor authentication early in the relationship and outside the e-mail environment to avoid interception by a hacker.
  - o Digital Signatures: Both entities on each side of a transaction should utilize digital signatures. This will not work with web-based e-mail accounts. Additionally, some countries ban or limit the use of encryption.
  - o Delete Spam: Immediately report and delete unsolicited e-mail (spam) from unknown parties. DO NOT open spam e-mail, click on links in the e-mail, or open attachments. These often contain malware that will give subjects access to your computer system.
  - o Forward vs. Reply: Do not use the "Reply" option to respond to any business e-mails. Instead, use the "Forward" option and either type in the correct e-mail address or select it from the e-mail address book to ensure the intended recipient's correct e-mail address is used.
  - o Consider implementing Two Factor Authentication (TFA) for corporate e-mail accounts. TFA mitigates the threat of a subject gaining access to an employee's e-mail account through a compromised password by requiring two pieces of information to login: something you know (a password) and something you have (such as a dynamic PIN or code).

67. Finally, as indicated by another PSA published by the FBI on May 4, 2017, entitled "Business Email Compromise E-Mail Account Compromise The 5-Billion Dollar Scam," e-mail

fraud schemes directed at businesses had increased by 61.3% since the time of the FBI's last update 10 months earlier, on June 14, 2016, which timeframe included the Accolade Data Disclosure.[22]

68. Based upon these explicit warnings by the IRS and FBI alone—particularly in combination with the numerous, similar data-breaches nationwide in recent months, Accolade was placed on notice that it needed to implement and maintain adequate and reasonable data security processes, controls, policies, procedures, and protocols to safeguard and protect the sensitive and confidential information with which it was entrusted.

69. Notwithstanding the security measures and protocols which should have been in place to prevent the unauthorized disclosure of PII, a simple phone call by Accolade's employee to confirm the identity of the third-party and to otherwise verify the request for PII would have prevented the unauthorized Data Disclosure.

70. Part of Accolade's day to day business is handling and protecting its client consumers' personal health information (or PHI), including client's medical information, prescriptions, partial social security numbers, address and other identifying information.

71. Accolade's employees, including Plaintiff, receive annual training regarding HIPPA requirements and other confidentiality requirements and are required to keep Accolade's client's information protected.

72. In fact, in a recent article about his book on digital forensics, Accolade's security director Mike Sheward stressed the importance of policies and procedures for security practices, noting "healthcare information we work with is highly sensitive, deeply personal and we owe it to

[22] See Business E-Mail Compromise E-Mail Account Compromise The 5 Billion Dollar Scam, Federal Bureau of Investigation, https://www.ic3.gov/media/2017/170504.aspx (last visited October 10, 2017).

our customers to keep it safe."[23] Sheward further commented that security incidents are more likely to be caused by a "person clicking on a phishing site" than other risks.

73. Despite Accolade's own awareness of the risks of phishing and daily handling of sensitive information of its customers' information, it failed to ensure that such protections were taken as to Plaintiff's and Class Members' PII. Indeed, although there was a well-known widespread prevalence of spoofing aimed at obtaining confidential information from employers and despite the warnings of the W-2 email scam from the 2015 tax season and renewed alerts for the 2016 tax season, Accolade provided its employees with unreasonably deficient training on cybersecurity and information transfer protocols prior to the Data Disclosure.

74. Accolade should have adequately trained its employees on even the most basic of cybersecurity protocols, including:

a. How to detect phishing and spoofing emails and other scams including providing employees examples of these scams and guidance on how to verify if emails are legitimate;

b. Effective password management and encryption protocols for internal and external emails;

c. Avoidance of responding to emails that are suspicious or from unknown sources;

d. Locking, encrypting and limiting access to computers and files containing sensitive information;

e. Implementing guidelines for maintaining and communicating sensitive data; and

f. Protecting sensitive employee information, including personal and financial

[23] https://www.geekwire.com/2017/mike-sheward/

information, by implementing protocols on how to request and respond to requests for the transfer of such information and how to securely send such information through a secure file transfer system to only known recipients.

75. Accolade's failures handed criminals the PII of Plaintiff and other Class Members and put Plaintiff and the Class at serious, immediate and ongoing risk for identity theft and fraud.

76. While there is a market for this PII for other long-term scams, the immediate and short-term practice with such breaches or compromises of PII is that the cyber criminals will use the PII to file false tax returns. Access to W-2 information permits identity thieves to quickly and easily file fraudulent tax returns, using the victim's information to obtain a fraudulent refund. The IRS will direct deposit the refund to the bank account or prepaid debit card (which are virtually untraceable) provided by the thief.

77. The Data Disclosure was caused by Accolade's violation of its obligation to abide by best practices and industry standards concerning the security of its computer and payroll processing systems. Accolade failed to comply with security standards and allowed its employees' PII to be compromised by failing to implement security measures that could have prevented or mitigated the Data Disclosure. Accolade failed to implement even the most basic of security measures to require encryption of any data file containing PII sent electronically, even internally within the company.

78. Accolade failed to ensure that all personnel in its human resources and payroll departments were made aware of this well-known and well-publicized phishing email scam.

79. Upon discovery, Accolade failed to provide detailed information to clearly and conspicuously inform Plaintiff and the other Class Members of the nature and extent of the Data Disclosure, leaving Plaintiff and Class Members only with the option of complimentary credit

monitoring, which does not and cannot explain or prevent the true scope of risk caused by the Data Disclosure.

80. The ramifications of Accolade's failure to keep its employees' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

81. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[24] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[25]

82. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

83. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later.[26]

84. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these

---

[24] 17 C.F.R. § 248.201 (2013).
[25] *Id.*
[26] Social Security Administration, Identity Theft and Your Social Security Number, *available at* http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited December 30, 2016).

fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

85. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security Number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

86. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[27]

87. Based on the foregoing, the information compromised in the Data Disclosure is significantly more valuable than the loss of, say, credit card information in a large retailer data breach such as those that occurred at Target and Home Depot. Victims affected by those retailer breaches could avoid much of the potential future harm by cancelling credit or debit cards and obtaining replacements.

88. Indeed, the Data Disclosure by Accolade was not a breach at all but instead the result of a compromise of Accolade's system resulting in the disclosure – by Accolade itself – of the sensitive PII.

---

[27] *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9, 2015, *available at* http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited December 31, 2016).

89. The information compromised in the Accolade Data Disclosure is difficult, if not impossible, to change—Social Security number, name, employment information, income data, etc.

90. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[28]

91. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police during an arrest.

92. The fraudulent activity resulting from the Data Disclosure may not come to light for years.

93. Despite all of the publicly available knowledge of the continued compromises of PII, alerts regarding the actual W-2 phishing email scam perpetrated, and Accolade's own business of protecting its customers' PHI, Accolade's approach to maintaining the privacy of its employees PII was lackadaisical, cavalier, reckless, or in the very least, negligent.

94. Accolade realized or should have realized the likelihood of such phishing attempts by unauthorized third-parties.

95. Accolade encountered a specific threat of intrusion into Plaintiff's and Class Members' PII when it received an email seeking highly sensitive PII. Rather than take measures to protect against such a threat, Accolade, through its agent, disclosed the PII without Plaintiff's and Class Members' consent.

---

[28] *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Tim Greene, Feb. 6, 2015, *available at* http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited December 29, 2016).

96. Accolade reasonably should have anticipated that such negligent handling of Plaintiff's and Class Members' PII – information which was otherwise confidential – left it vulnerable to criminal activity, like phishing.

97. Indeed, the receipt of the email seeking Plaintiff's and Class Members' PII put Accolade on notice of a potential threat to the security of the PII and it failed to take adequate measures to ensure the authenticity of the outside request for information.

98. The criminal acts of third-parties in sending the phishing email does not absolve Accolade from its voluntary disclosure and dissemination of its employees' PII without their authorization.

99. Accolade has failed to provide compensation to Plaintiff and Class Members victimized in this Data Disclosure. Accolade has not offered to provide any compensation for the costs and burdens – current and future - associated with the identity theft and fraud resulting from the Data Disclosure. Accolade has not offered employees any assistance in dealing with the IRS or state tax agencies.

100. It is incorrect to assume that reimbursing a consumer for financial loss due to fraud makes that individual whole again. On the contrary, after conducting a study, the U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims." [29]

101. To date, Accolade has offered its employees only one year of credit monitoring service through Experian's ProtectMyID Alert Program. The offered service is inadequate to

[29] Victims of Identity Theft, 2012 (Dec. 2013) at 10, 11, *available at* https://www.bjs.gov/content/pub/pdf/vit12.pdf (last visited December 8, 2017).

protect the Plaintiff and Class Members from the threats they face, particularly in light of the PII stolen. Experian has actually suffered its own data breach, and there is no assurance that it can be trusted with PII and sensitive information.

102. Plaintiff's and Class Members' PII is an intangible asset that has value. PII like that which was disclosed by Accolade is lawfully sold by companies like Experian and others for use in target marketing, etc. There is also a substantial likelihood that Plaintiff's PII has been monetized and sold by third-parties on the dark web.

103. Because of Accolade's Data Disclosure, the PII is no longer valuable to Plaintiff and Class Members as it once was.

104. As a result of Accolade's failures to prevent the Data Disclosure, Plaintiff and Class Members have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety and emotional distress.

105. They have suffered:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise, publication and/or theft of their PII;

106. They are also at increased risk of suffering or have already been harmed by:

a. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud, including credit freezes and/or credit monitoring;

b. Lost opportunity costs and lost wages associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Disclosure, including but not limited to efforts spent

researching how to prevent, detect, contest and recover from identity theft and fraud;

c. Delay in receipt of tax refund monies;

d. Unauthorized use of compromised PII;

e. The continued risk to their PII, which remains in the possession of Accolade and is subject to further compromises from phishing schemes so long as Accolade fails to undertake appropriate measures to protect the PII in their possession; and

f. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Disclosure for the remainder of the lives of Plaintiff and Class Members.

CLASS ACTION ALLEGATIONS

107. Plaintiff brings this suit as a class action on behalf of herself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), (b)(3) and (c)(4) of the Federal Rules of Civil Procedure.

108. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> All current and former U.S.-based Accolade employees whose PII was compromised as a result of the Data Disclosure.

109. In the alternative to the Nationwide Class, and pursuant to Federal Rule of Civil Procedure 23(c)(5), Plaintiff seeks to represent the following state classes only in the event that the Court declines to certify the Nationwide Class above. Specifically, the state classes consist of the following:

> All current and former U.S.-based Accolade employees who currently reside in Pennsylvania and whose PII was compromised as a result of the Data Disclosure.

110. Excluded from the Class are the officers, directors and legal representatives of Accolade and the judges and court personnel in this case and any members of their immediate families.

111. Numerosity. Fed. R. Civ. P. 23(a)(1). The members of the Class are so numerous that joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiff at this time, based on information and belief, it is estimated to be at or above 500. The exact number is generally ascertainable by appropriate discovery as Accolade had knowledge of the employees whose PII was in the data file it disclosed.

112. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether and to what extent Accolade had a duty to protect the PII of Class Members;

b. Whether Accolade failed to adequately safeguard the PII of Class Members;

c. Whether Accolade adequately, and accurately informed Class Members that their PII had been compromised;

d. Whether an implied contract existed between Defendant and the Class and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Accolade failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Disclosure;

g. Whether Accolade engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Class Members;

h. Whether Class Members are entitled to actual, damages, statutory damages, and/or punitive damages as a result of Accolade's wrongful conduct;

a. Whether Plaintiff and the members of the Class are entitled to restitution as a result of Accolade's wrongful conduct; and,

b. Whether Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Disclosure.

113. Typicality. Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other class member, was disclosed by Accolade. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Members of the Class were injured through the common misconduct of Defendant. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other Class members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of other Class members arise from the same operative facts and are based on the same legal theories.

114. Adequacy of Representation. Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of the Class in that they have no disabling conflicts of interest that would be antagonistic to those of the other members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class members. Plaintiff has retained counsel experienced in complex consumer class action litigation, and Plaintiff intends to prosecute this action vigorously.

115. Superiority of Class Action. Fed. R. Civ. P. 23(b)(3). The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain class members, who could not individually afford to litigate a complex claim against large corporate Accolade. Further, even for those class members who could afford to litigate such a claim, it would still be economically impractical.

116. The nature of this action and the nature of laws available to Plaintiff and the Class make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and the Class for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each member of the Class to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

117. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class

Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

118. Adequate notice can be given to Class Members directly using information maintained in Accolade's records.

119. Unless a Class-wide injunction is issued, Accolade may continue in its failure to properly secure the PII of Class Members, Accolade may continue to refuse to provide proper notification to Class Members regarding the Data Disclosure, and Accolade may continue to act unlawfully as set forth in this Complaint.

120. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the members of the Class as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

121. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Defendant failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

FIRST CAUSE OF ACTION
Breach of Implied Contract

(On Behalf of the Class)

122. Plaintiff restates and realleges paragraphs 1-106 above as if fully set forth herein.

123. Plaintiff and Class members were required to provide their PII, including names, addresses, Social Security numbers, and other personal information, to Accolade as a condition of their employment.

124. Implicit in the employment agreement between the Accolade and its employees was the obligation that both parties would maintain information confidentially and securely.

125. Accolade had an implied duty of good faith to ensure that the PII of Plaintiff and Class members in its possession was only used to provide agreed-upon compensation and other employment benefits from Accolade.

126. Accolade had an implied duty to reasonably safeguard and protect the PII of Plaintiff and Class members from unauthorized disclosure or uses.

127. Additionally, Accolade implicitly promised to retain this PII only under conditions that kept such information secure and confidential.

128. Plaintiff and Class members fully performed their obligations under the implied contract with Accolade. Accolade did not.

129. Plaintiff and Class members would not have provided their confidential PII to Accolade in the absence of their implied contracts with Accolade, and would have instead retained the opportunity to control their PII for uses other than compensation and employment benefits from Defendant.

130. Accolade breached the implied contracts with Plaintiff and Class members by failing to reasonably safeguard and protect Plaintiff's and Class members' PII, which was

compromised as a result of the Data Disclosure.

131. Accolade's acts and omissions have materially affected the intended purpose of the implied contacts requiring Plaintiff and Class members to provide their PII as a condition of employment in exchange for compensation and benefits.

132. As a direct and proximate result of Accolade's breach of its implied contacts with Plaintiff and Class members, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) the loss of the opportunity how their PII is used; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Disclosure, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes and/or credit monitoring on credit reports; (vi) the continued risk to their PII, which remain in Accolade's possession and is subject to further unauthorized disclosures so long as Accolade fails to undertake appropriate and adequate measures to protect the PII of employees and former employees in its continued possession; and, (vii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Disclosure for the remainder of the lives of Plaintiff and Class members.

SECOND CAUSE OF ACTION
Negligence
(On Behalf of the Class)

133. Plaintiff restates and realleges paragraphs 1-106 above as if fully set forth herein.

134. Plaintiff's and Class Members' PII was compromised as a result of Accolade's

negligence.

135. As a condition of their employment, employees were obligated to provide Accolade with certain PII, including their date of birth, mailing addresses and Social Security numbers.

136. Plaintiff and the Class Members entrusted their PII to Accolade on the premise and with the understanding that Accolade would safeguard their information.

137. Plaintiff and the Class Members entrusted Accolade with their PII with the understanding that Accolade would safeguard and protect their information, and that Accolade was in a position to safeguard and protect against the harm suffered by Plaintiff and the Class Members as a result of the Data Disclosure.

138. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

139. Defendant had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining and testing Defendant's security protocols to ensure that Plaintiff and Class members' information in its possession was adequately secured and protected and that employees tasked with maintaining such information were adequately training on cyber security measures regarding the security of employees' personal and tax information. Accolade knew that by collecting and storing its employees' sensitive, personal and financial information, it undertook such a responsibility. Accolade owed such a duty of care to Plaintiff and the Class Members because they were foreseeable and probable victims of any inadequate security practices. Plaintiff and the Class Members had no ability to protect their data that was in Accolade's possession.

140. Plaintiff and the Class Members were the foreseeable and probable victims of any

inadequate security practices and procedures. Accolade knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, the current cyber scams being perpetrated on companies, and that it had inadequate employee training and education and IT security protocols in place to secure the PII of Plaintiff and the Class.

141. Accolade's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Accolade's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Disclosure as set forth herein. Accolade's misconduct also included its decision not to comply with industry standards for adequate safekeeping and encryption of the PII of Plaintiff and Class Members.

142. Plaintiff and the Class Members had no ability to protect their PII that was in Accolade's possession.

143. Accolade was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Disclosure.

144. Accolade had and continues to have a duty to adequately disclose that the PII of Plaintiff and Class Members within its possession might have been compromised, how it was compromised and precisely the types of information that were compromised and when. Such notice was necessary to allow Plaintiff and the Class Members to take steps to prevent, mitigate and repair any identity theft and the fraudulent use of their PII by third parties.

145. Accolade had a duty to have proper procedures in place to prevent the unauthorized dissemination of the PII of Plaintiff and Class Members.

146. Accolade has admitted that the PII of Plaintiff and Class Members was wrongfully disclosed to unauthorized third persons as a result of the Data Disclosure.

147. Accolade, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding the PII of Plaintiff and Class Members during the time the PII was within Accolade possession or control.

148. Accolade improperly and inadequately safeguarded the PII of Plaintiff and Class Members in deviation of standard industry rules, regulations and practices at the time of the Data Disclosure.

149. Accolade failed to heed industry warnings and alerts issued by the IRS to provide adequate safeguards to protect employees' PII in the face of increased risk of a current phishing email scheme being perpetrated.

150. Accolade, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its employees' PII.

151. Accolade, through its actions and/or omissions, unlawfully breached its duty to adequately disclose to Plaintiff and Class Members the existence, and scope of the Data Disclosure.

152. But for Accolade's wrongful and negligent breach of duties owed to Plaintiff and Class Members, the PII of Plaintiff and Class Members would not have been compromised.

153. There is a close causal connection between Accolade's failure to implement security measures to protect the PII of current and former employees and the harm suffered or risk of imminent harm suffered by Plaintiff and the Class.

154. As a result of Accolade's negligence, Plaintiff and the Class Members have suffered and will continue to suffer damages and injury including, but not limited to: out-of-pocket

expenses associated with credit freezes and/or credit monitoring; fees incurred in seeking professional advice regarding the Data Disclosure; expenses associated with addressing any false tax returns filed; current and future out-of-pocket costs in connection with preparing and filing tax returns; loss or delay of tax refunds as a result of fraudulently filed tax returns; out-of-pocket expenses associated with procuring robust identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing and correcting the current and future consequences of the Data Disclosure.

155. Plaintiff and the Class Members also have suffered and will continue to suffer emotional distress as a result of the fear and anxiety regarding how their stolen PII will be used to their detriment.

156. Plaintiff and the Class Members also have suffered and will continue to suffer from the damage to and reduced value of their PII which has been irreparably harmed and compromised as a result of Defendant's conduct.

THIRD CAUSE OF ACTION
Negligence Per Se
(On Behalf of the Class)

157. Plaintiff restates and realleges paragraphs 1-106 above as if fully set forth herein.

158. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses of failing to use reasonable measures to protect PII.

159. Accolade violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Accolade's conduct was particularly unreasonable and unconscionable given the nature and amount of PII it obtained and stored, on behalf of both its customers and employees, and the

foreseeable consequences of disclosing PII in response to an unsolicited phishing attempt by a third-party. The immense damages that would result to Plaintiff and Class Members as a result of the Data Disclosure was equally foreseeable.

160. Accolade's violation of Section 5 of the FTC Act constitutes negligence *per se*.

161. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

162. The harm that occurred as a result of the Data Disclosure is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

163. As a direct and proximate result of Accolade's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, injuries damages arising from Plaintiff's and the Class's inability to use debit or credit cards or limited use of debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Disclosure and/or false or fraudulent charges stemming from the Data Disclosure, including but not limited to late fees charges and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Disclosure on their lives including, inter alia, by monitoring credit reports and/or placing "freezes" and "alerts" through credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

164. Plaintiff and the Class Members also have suffered and will continue to suffer emotional distress as a result of the fear and anxiety regarding how their stolen PII will be used to their detriment.

165. Plaintiff and the Class Members also have suffered and will continue to suffer from the damage to and reduced value of their PII which has been irreparably harmed and compromised as a result of Defendant's conduct.

FOURTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of the Class)

166. Plaintiff restates and realleges paragraphs 1-106 above as if fully set forth herein.

167. Accolade was a fiduciary, as an employer created by its undertaking, to act primarily for the benefit of its employees, including Plaintiff and Class members, for the safeguarding of employees' PII and wage information.

168. Accolade had a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of their employer/employee relationship, in particular to keep secure income records and the PII of its employees.

169. Accolade breached its duty of care to Plaintiff and Class members to ensure that their PII and W-2 data was not disclosed without authorization or used for improper purposes by failing to provide adequate protections to the information and by voluntarily disclosing the information, in an unencrypted format, to an unknown and unauthorized third party.

170. As a direct and proximate result of Accolade's actions alleged above, Plaintiff and Class members have suffered actual damages, including, but not limited to: out-of-pocket expenses associated with credit freezes and/or credit monitoring or fees incurred in seeking professional

advice regarding the Data Disclosure; expenses associated with addressing any false tax returns filed; current and future out-of-pocket costs in connection with preparing and filing tax returns; loss or delay of tax refunds as a result of fraudulently filed tax returns; out-of-pocket expenses associated with procuring robust identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing and correcting the current and future consequences of the Data Disclosure.

171. As a result of Defendant's breach of fiduciary duty, Plaintiff and the Class Members also have suffered and will continue to suffer emotional distress as a result of the fear and anxiety regarding how their stolen PII will be used to their detriment.

172. Plaintiff and the Class Members will continue to suffer from the damage to and reduced value of their PII which has been irreparably harmed and compromised as a result of Defendant's conduct.

PRAYER FOR RELIEF

WHEREFORE Plaintiff on behalf of herself and all others similarly situated, pray for relief as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and her Counsel to represent the Class;

B. A mandatory injunction directing Accolade to hereinafter adequately safeguard the PII of the Class by implementing improved security procedures and measures;

C. A mandatory injunction requiring that Accolade provide notice to each member of the Class relating to the full nature and extent of the Data Disclosure and the disclosure of PII to unauthorized persons;

D. For an award of damages, in an amount to be determined;

E. For an award of attorneys' fees and costs;

F. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: January 22, 2018

Respectfully submitted,

Charles E. Schaffer
Daniel C. Levin
LEVIN SEDRAN & BERMAN
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Telephone: (215) 592-1500
Facsimile: (215) 592-4663
cschaffer@lfsblaw.com
dlevin@lfsblaw.com

STECKLER GRESHAM COCHRAN PLLC
Bruce W. Steckler (*pro hac vice forthcoming*)
Texas Bar No. 00785039
L. Kirstine Rogers (*pro hac vice forthcoming*)
Texas Bar No. 24033009
12720 Hillcrest Road – Suite 1045
Dallas, TX 75230
Telephone: 972-387-4040
Facsimile: 972-387-4041
bruce@stecklerlaw.com
krogers@stecklerlaw.com

MORGAN & MORGAN
John A. Yanchunis (*pro hac vice forthcoming*)
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402
jyanchunis@ForThePeople.com